UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/633,816	08/04/2003	Leon Pryor	MS1-1626US	7499

22801 7590 07/22/2008
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
SHAH, MILAP	
ART UNIT	PAPER NUMBER
3714	
MAIL DATE	DELIVERY MODE
07/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/633,816	PRYOR, LEON	
	Examiner	Art Unit	
	Milap Shah	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-7,9-11,13-23,25-27,30-35 and 38-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-7,9-11,13-23,25-27,30-35 and 38-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/14/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on May 12, 2008 has been entered.

The Examiner acknowledges that claims 1, 17, 23, 30-33, 38, & 39 were amended, claims 28, 29, 36, & 37 were canceled, and no new claims were added. Therefore, claims 1, 3-7, 9-11, 13-23, 25-27, 30-35, & 38-41 are currently pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3-7, 9-11, 13-23, 25-27, 30-35, & 38-41 are rejected under 35 U.S.C. 102(b) as being anticipated by "Security Issues in Online Games" by Jianxin Jeff Yan & Hyun-Jin Choi (hereafter "Yan et al."). Note: This non-patent literature was provided with a prior office action dated March 31, 2006.

Examiner Note: In the following rejection, the Examiner has cited particular citations in the reference as applied to the claims for convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other citations and figures may apply as well. Thus, it is respectfully requested that

the Applicant, in preparing any response to this communication, fully consider the reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passages as taught by the prior art or disclosed by the Examiner. The Examiner is also required to give broad claim limitations their broadest reasonable interpretation in light of the ordinary level of skill in the respective art.

Claims 1, 3-5, 7, 13, 17, 18, 23, 25, 32, & 33: Yan et al. disclose the same invention including monitoring players in a game (automatically via cheat detection engine), wherein the game is monitored only on a game server (page 130, section C-1 discloses that in the case that game designers cannot provide guaranteed security for game clients, the built-in cheat detection engine should be implemented in the game server where it is difficult for cheaters to tamper with the software, thus providing a teaching of having a built-in cheat detection engine within only the game server), based on said monitoring, identifying one or more player-exploitable game conditions, where the player exploitable game conditions are programming conditions situations or aberrations produced within the game that give one or more cheating players an advantage without the cheating player hacking the game, wherein the player-exploitable game conditions are identified by observing the players' play of the game (page 130, section C-1 discloses a popular item duplication cheat and discusses that game behavior can be monitored such that when gaming behavior violates certain principles or thresholds, a built-in triggering event will take appropriate action, thus providing a teaching of identifying the player-exploitable game conditions, sections B-3 and B-11 also disclose various player exploitable game conditions that can be used for cheating), setting a threshold against which the player of the players is compared, wherein the threshold is set based on a rate at which virtual property is acquired during the play and wherein the threshold is configured to be modified in real time during game play (page 130, section C-1 discloses "...the number of items generated by the system should always be equal to the number of items that are possessed and consumed by all

the player. Therefore, when a gaming behavior violates this principle, a triggering event will be thrown to the built-in detection engine, which will take the appropriate actions", which appears to teach or imply that a threshold is dynamically set in real time based on the number of players within the game and the total number of items consumed or possessed by those game players. Additionally since the total number of players constantly changes in online games of the type being discussed at page 130, section C-1, the triggering event would require a threshold that changed in real-time with the changes in game play, number of players, and virtual property, thus, it could be further seen that such a feature/limitation is inherent to the disclosure), and identifying, among the players, one or more cheating players who are exploiting the player-exploitable game conditions, the identifying comprising comparing the rates at which the cheating players acquire virtual property in the game against the threshold, whereby the cheating players and player-exploitable game conditions are dealt with to prevent from further occurrence (page 130, section C-1 discloses the appropriate actions as discussed above once cheating is identified is to void the game change that the cheating behavior would like to achieve and record the cheater's ID, thus the cheating player and player-exploitable game conditions are identified and "dealt with"). See also the *Ultima Online* example at page 130, section C-1, which provides further evidence of monitoring game play versus thresholds, where the thresholds are set based on game play (i.e. based on virtual property in the game, virtual money in the game, etc…).

Regarding claim 17, the above method is considered to be carried out within a game server, which is a general computer having a processor or CPU, one or more computer readable media (memory), and where the processor is configured to carry out the cheat detection process as described above.

Regarding claims 5, 13, 23, & 33 all of the above appears to apply and additionally Yan et al. disclose determining whether the threshold is exceeded for any of the players of the game at least

based on the disclosure at page 130, section C-1 which states that if the "principle" (i.e. threshold) is exceeded, appropriate actions will be taken. Furthermore, Yan et al. also disclose logging the player of the player whose play exceeds the threshold to computer storage medium (i.e. where else would it go, if it's being logged/stored it would reside on some type of memory) at least based on the disclosure at page 131, section C-7 that discusses logging each game as a session record helps guarantee fairness. Based on this disclosure it can be seen that all play is logged, thus the player whose play exceeds the threshold (i.e. suspected cheats) is also logged in this situation. The logging is considered to encompass all of the game events and variable changes, thus, the logging is used, at least in part, by the detection system to determine or identify cheating players based on the logged play. Further in regard to claim 23, the player exploitable game condition being at least a dupping situation is disclosed by Yan et al., where dupping is considered to be another term for "item duplication" that Yan et al. disclose as discussed above. Item duplication provides cheating players with an unfair advantage by exploiting such a situation without hacking the game where such item duplication cheat is an exploit as discussed by Yan et al. (section B-11) that can be taken advantage of by a player.

Regarding claim 32, all of the above appears to apply and additionally it is readily apparent that the computer program or code to carry out the method discussed above is stored on a computer-readable medium so the game server is able to execute the game software (page 130, section C-1 discloses the built-in cheat detection engine is within the game software). Further in regard to claim 32, the player exploitable game condition being at least a dupping situation is disclosed by Yan et al., where dupping is considered to be another term for "item duplication" that Yan et al. disclose as discussed above. Item duplication provides cheating players with an unfair advantage by exploiting such a situation without hacking the game where such item duplication

cheat is an exploit as discussed by Yan et al. (section B-11) that can be taken advantage of by a player.

Claim 6: The item duplication player-exploitable game condition as discussed above would inherently provide a player who is duplicating an item, such as a weapon item, an advantage against other players.

Claims 9 & 11: Yan et al. disclose an active complain-response channel or system to let players of a game complain to game operators about potential security threats or information related to specific cheaters, in return, the game operators may send responses to those who've complained and cheaters who've been named (page 131, section C-6). Yan et al. disclose reporting "possible cheatings" to cheaters and other players, which may be considered reporting the actual activities the suspected cheater conducted to be labeled a cheater.

Claim 10: Yan et al. disclose security protocols that may disconnect a client if a validation process fails and the client is suspected of cheating (page 129, section B-10).

Claim 14: A popular player-exploitable game condition is a glitch in a map, level, or scene of a gaming virtual world. Glitches in maps include invisible spots which should be nothing, but end up being a hard platform that a character or player in a game is able to stand on, which puts that player at some location other than the ground plane in the virtual scene. One quick example is the game "Quake 2" which has a map called "The Edge" that has a map glitch which lets a player go to a specific spot in the map and enables the player to essentially "sky walk" and makes the player appear as though he's walking through the air. The map glitch is considered a player exploitable game condition, thus map glitches are inherently player exploitable game conditions since they are capable of allowing a player to be at some location other than the ground plane in the virtual scene. A threshold is capable of being set in a similar manner to the rate at which virtual property is consumed, such that if a player's position goes beyond a wall or ceiling position, then clearly the

player is cheating (see page 130, section B-11, which discusses bugs or design flaws; map glitches would be considered a bug or design flaw).

Claims 15 & 16: Yan et al. disclose the player-exploitable game conditions include a scoring cheat, such that some cheaters may stealthily remove live stones instead of dead stones from within a game known as Go (also known as WeiQi or Baduk) overturning the results (page 127, section B-2 & page 131, section C-7). Yan et al. disclose that money or expense exploits are within virtual assets cheating and where there is virtual money or expenses, there are cheaters trying to exploit the game to gain money in the virtual world (page 128, section B-3). Thus, these types of player-exploitable game conditions can be monitored in a similar manner as to the above discussion (i.e. thresholds for score and expense versus length of game play).

Claim 19: According to Applicant's specification an "asynchronous activity pump" provides desired game data relating to the play of the players in a game to the "play monitor". Yan et al. disclose a built-in detection portion which monitors game events and variables (page 130, section C-1), which is considered to be an "asynchronous activity pump" to provide the gaming events and variables to the detection portion (which is considered the play monitor).

Claim 20: The criteria met for logging to take place is simply that the player is playing the game in which logging is present.

Claims 21 & 22: Yan et al. disclose the built-in detection engine should be implement in a game server (page 130, section C-1) which the client or player is connected to through a network, thus the detection engine is included as a portion of a network. The server is also considered a "stand-alone computer system" since it is not considered dependent on any other system.

Claims 26 & 34: Yan et al. inherently disclose that a threshold can be "reset", at least in the situation when the game server reboots, it would appear that the threshold must start at some default value.

Claims 27 & 35: The above discussion includes various these types of player-exploitable game conditions, such that any of these player-exploitable game conditions that are conditions or situations produced without hacking the game are monitored based on the built-in cheat detection engine disclosed by Yan et al. These conditions relate to a player's virtual property (i.e. item duplication), a rollover rate, virtual money, and/or game score. Thus, it can be seen (as partially discussed above), that the built-in cheat detection can, based on the disclosure of Yan et al., provide thresholds for each type of player-exploitable game condition so that cheating players can be identified for exceeding thresholds related to the virtual property (i.e. item duplication), a rollover rate, virtual money, and/or game score (see page 127, section B-3 discussing cheating related to virtual assets which includes each of these three types of player-exploitable game conditions that page 130, section C entitled "Cheating mitigation: prevention, detection, and management" is trying to eradicate).

Claims 30, 31, 38, & 39: Yan et al. disclose that when cheating is detected, post-detection mechanisms are needed to punish identified cheaters. Cheaters should be punished and victims that were damaged unfairly in the game caused by the cheating should have their assets, score, or the like restored (page 131, section C-8). Thus, Yan et al. discloses punishing of cheaters and modifying the game to restore any losses accrued by the victims of the cheating incident.

Claims 40 & 41: Yan et al. disclose a built-in cheat detection system at the server level, as discussed above. Yan et al. explain that virtual assets are a big area in which exploiting is used. The built-in detection system disclosed monitors every game event and game variables (page 130, section C-1), thus, it is considered to monitor every item accrued, traded, lost, gained, etc. in a virtual world and indicate this to the player monitor (the built-in detection portion) so that a determination can be made by the built-in detection portion as to whether a player-exploitable game condition is being exploited. With regard to claim 41, the process is considered to be executed or carried out via

computer programming that is stored on a computer-readable storage medium and executed by a processor on the game server.

Response to Arguments

Applicant's arguments filed April 10, 2008 have been fully considered but they are not persuasive. The Applicant argues that Yan et al. do not anticipate the claimed invention. The Examiner respectfully disagrees.

First, the Examiner submits that section B of Yan et al., parts 1-11 discuss various methods of cheating and section C, parts 1-6 discuss ways to mitigate, prevent, detect and manage cheating behaviors. Thus, initially the Examiner submits that the Applicant's analysis of Yan et al. is in error, at least in terms that the Applicant asserts the built-in cheat detection does not identify player exploitable game conditions. Yan et al. provide multiple cheating scenarios and multiple scenarios to mitigate, prevent, detect, or manage the various cheating scenarios. Thus, those skilled in the art would possess the knowledge to utilize the disclosure as a whole to select a suitable one of the cheat mitigation, prevent, detection, or management schemes discussed by Yan et al. to avoid cheating by one of the cheating types discussed by Yan et al.; thus, it appears anticipatory given the Yan et al. disclosure to prevent cheating based on exploits without hacking the game utilizing a built-in cheat detection means to monitor various game events and variables for a cheating behavior.

At paragraphs 0018-0022, the Applicant argues that Yan et al. do not teach or disclose "identifying comprising comparing the rates at which the cheating players acquire the virtual property in the game against "the threshold" and further support the argument with Yan's discussion of the Ultima Online game. It should be noted that section C-1 contains many examples of built-in cheat detection, where Ultima Online is merely one example. The Examiner also relied on the preceding paragraph of Yan et al., in the rejection. Yan et al. disclose "a popular cheat of item duplication as an example, the number of items

generated by the system should always be equal to the number of items that are possessed and consumed by all players" and further discloses "when a game behavior violates this principle, a triggering event will be thrown to the built-in detection engine, which will take appropriate actions, e.g. void the game chance that the cheating behavior would like to achieve, and record the cheater's ID". In combination with known cheating methods discussed in section B, specifically in section B-11, "cheat by exploiting bugs or design flaws", those of ordinary skill would find it anticipatory that the built-in cheat detection engine monitors play of the game and identifies based on that play cheating players by comparing the rates at which these players acquire virtual property against a threshold. Clearly, the rate is the number of items obtained, created, or the like and the threshold is disclosed by Yan et al. in that the number of items generated by the system must be equal to the number of items that are possessed and consumed by all players. Thus, when such a threshold has been exceeded, Yan et al. clearly disclose dealing with the cheating players, for example, by voiding the game change and logging the player's ID. Yan et al., in section C makes no specific disclosure as to what type of cheating would trigger such cheat detection or prevention counter measures. Thus, such cheating behavior could be any one of hacking the game or a player finding an exploitable game condition without hacking the game. Upon either hacking or an exploit, duplication of the virtual assets would be detected by the built-in detection system. Therefore, the Examiner submits that Yan's acknowledgement of player exploitable game conditions without hacking the game in section B-11, and Yan's counter measures to detect any type of cheating for at least item duplication, anticipates the claimed invention.

At paragraphs 0024-0027, the Applicant asserts that the context of section C-1 shows that Yan et al. is focused on built-in cheat detection when traditional security mechanisms are comprised due to hacker intrusions. The Applicant further argues "The Applicant reasonably assumes that the built-in cheating detection is used to prevent hacker intrusions". The Examiner respectfully disagrees with this analysis. The sentence that the Applicant has cited discusses an intrusion detection system (i.e. a firewall or the like) at the server side to prevent hackers from attacking the server, while the same sentence discusses a built-in cheat

detection engine as one built into the game software to prevent many cheating behaviors by monitoring critical game events and variables. One such variable would be the variables or parameters associated with the virtual property. Further, Yan et al. also disclose that this built-in cheat detection system could be implemented in the game software that each client uses or a built-in cheat detection system implemented in the game software that operates the online game on the game server, where it is difficult for cheaters or hackers to tamper with the game software. Lastly, as acknowledged by Yan et al. there are numerous types of cheating that have nothing to do with hacking or altering game software or game servers (see section B). Yan et al. also disclose cheating in regards to virtual assets or property that is done via player exploitable game conditions or situations that have nothing to do with hacking the game (see section B-4 in regards to trade cheating). It is noted that Yan et al. disclose that the "practical solution" for player exploitable game conditions is to patch such conditions; however, this disclosure does not preclude such game conditions from being *identified* by a built-in cheat detection engine disclosed by Yan et al.

For at least the reasons discussed above, the Examiner submits that, given the Yan et al. reference as a whole, those of ordinary skill in the art would have anticipated the claimed invention as each and every limitation appears to be disclosed either explicitly or inherently by Yan et al. Those skilled in the art would posses the ordinary skill to utilize the various cheat prevention, mitigation, detection, and management methods disclosed in section C against any possible cheating method of at least the ones disclosed in section B, such as exploits. Lastly, it should be noted that using exploits to one's advantage is a well known "cheating" method in gaming industry.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Milap Shah whose telephone number is (571)272-1723. The examiner can normally be reached on M-F: 9:30AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert Pezzuto can be reached on (571) 272-6996. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Robert E Pezzuto/
Supervisory Patent Examiner, Art Unit 3714

/MBS/